UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/655,803	09/06/2000	KAZUNORI HORIKIRI	107196	9505

25944 7590 08/09/2005

OLIFF & BERRIDGE, PLC
P.O. BOX 19928
ALEXANDRIA, VA 22320

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/655,803	HORIKIRI, KAZUNORI	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 May 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 12-19* is/are pending in the application.

4a) Of the above claim(s) *15-19* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 12-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 October 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/11/00*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response to restriction filed on 20 May 2005 has been noted and made of record, Group I has been elected.

2. Claims 1-10 and 12-14 have been presented for examination.

Response to Arguments

3. Applicant's arguments with respect to claims 1-10 and 12-14 have been considered but are moot in view of the new ground(s) of rejection.

4. See further rejections that follow.

Claim Rejections

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 2, 4, 5, 10, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,330,677 to Madoukh, hereinafter Madoukh, in view of U.S. Patent No. 6,292,790 to Krahn et al., hereinafter Krahn.

8. As per claims 1 and 10, Madoukh teaches an access privilege transferring method for safely transferring access privileges between clients, and between clients and servers, over an object space in which at least one server for providing objects and at least one client requiring the objects are connected to one another by a network, and access to each of the objects complying with privilege information held by each of the clients is allowed, comprising:

holding, user information and secret information by each of a plurality of clients (Figure 1 [blocks 104, 114], 2 [step 204], 6 [step 244], 11 [blocks 1104], column 3, line 62 to column 4, line 3, column 4, lines 29-51, column 5, lines 18-40);

holding, in a server, the user information and the secret information of at least a first of the plurality of the clients (Figure 1 [block 124], 3 [step 218], 7 [step 262], 11 [blocks 1122, 1123], column 3, line 62 to column 4, line 3, column 4, line 51 to column 5, line 18, column 5, lines 28-51);

generating privilege information by the at least the first of the plurality of clients (Figure 2 [step 208], 3 [steps 214, 216], 6 [steps 246, 248], 7 [steps 258, 260], column 4, lines 42-63, column 5, lines 18-40);

applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege information by the at least the first of the plurality of clients (Figure 2 [step 208], 3 [steps 214, 216], 6 [steps 246, 248], 7 [steps 258, 260], column 4, lines 42-63, column 5, lines 18-40);

transmitting the user information, the privilege information and the protected privilege information from the at least the first of the plurality of clients to at least a second of the plurality of clients (Figure 9 [block 286], column 5, line 62 to column 6, line 12);

retransmitting, from the at least the second of the plurality of clients the user information, the privilege information and the protected privilege information to the server, thereby making a request to access an object (Figure 9 [block 288], column 5, line 62 to column 6, line 12);

checking, by the server, whether the privilege information received from the at least the second of the plurality of clients is valid (column 6, lines 29-47);

comparing the protected privilege information received by the server with the protected privilege-information generated by the server (Figure 9 [steps 290, 292], column 5, line 62 to column 6, line 12); and

allowing access to an object in response to the coincidence of the received protected privilege information and the generated protected privilege information based on the results of the comparison (Figure 9 [step 296], column 6, lines 9-28, column 14, lines 3-51, i.e. accessing objects via the object request broker).

9. Madoukh does not disclose applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege by the server.

10. Krahn teaches hashing a password and comparing it against stored hashed passwords (column 1, line 53 to column 2, line 13).

11. It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply a predetermined calculation to the information (i.e. one-way hash) and comparing the protected information with the generated protected information, since Krahn states at column 2, lines 9-12 that the server does not store plain-text passwords, thereby preventing unauthorized access from obtaining every user's password.

12. Regarding claims 2 and 7, Madoukh discloses wherein the at least the second of the plurality of clients retransmits the user information, the privilege information and the protected privilege information to at least a third of the plurality of clients (Figure 9 [block 288], column 5, line 62 to column 6, line 12).

13. As per claims 4 and 12, Madoukh discloses an access privilege transferring method for allowing each of the servers activated over an object space in which at least one server for providing objects and at least one client requiring the objects are connected to one another by a network and access to each of the objects based on privilege information held by each of the clients is allowed to safely respond to an access request issued from the client to which access privileges are transferred, comprising:

receiving an access request including user information, privilege information and protected privilege information ();

checking whether the received privilege information is valid (Figure 9 [block 288], column 5, line 62 to column 6, line 12);

comparing the received protected privilege information with the generated protected privilege information (Figure 9 [steps 290, 292], column 5, line 62 to column 6, line 12); and

allowing access to an object in response to the coincidence of the received protected privilege information and the generated protected privilege information based on the results of the comparison (Figure 9 [step 296], column 6, lines 9-28, column 14, lines 3-51, i.e. accessing objects via the object request broker).

14. Madoukh does not disclose applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege by the server.

15. Krahn teaches hashing a password and comparing it against stored hashed passwords (column 1, line 53 to column 2, line 13).

16. It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply a predetermined calculation to the information (i.e. one-way hash) and comparing the protected information with the generated protected information, since Krahn states at column 2, lines 9-12 that the server does not store plain-text passwords, thereby preventing unauthorized access from obtaining every user's password.

17. Regarding claims 5 and 9, Krahn teaches wherein applying a predetermined calculating operation further comprises applying a one-way function to a bit string obtained by concatenating operands with one another (column 1, line 53 to column 2, line 13).

18. Claim 3 is rejected under 35 U.S.C. 102(e) as being anticipated by Madoukh.

19. As per claim 3, Madoukh teaches an access privilege transferring method for allowing each of the clients activated over an object space in which at least one server for providing objects and at least one client requiring the objects are connected to one another by a network and access to each of the objects complying with privilege information held by each of the clients is allowed to safely transfer access privileges to another client, comprising:

holding user information and secret information to be shared by at least the one server (Figure 1 [block 124], 2 [block 202], 3 [step 218], 7 [step 262], 11 [blocks 1122, 1123], column 3, line 62 to column 4, line 3, column 4, line 51 to column 5, line 18, column 5, lines 28-51);

generating privilege information (Figure 4 [block 232], column 5, lines 7-17); and

applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege information to be safely transferred to a client (Figure 5 [blocks 234, 236], column 5, lines 7-17).

20. Claims 6-9, 13, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Madoukh in view of Krahn, and further in view of U.S. Patent No. 6,173,400 to Perlman et al., hereinafter Perlman.

21. As per claims 6 and 13, Madoukh teaches an access privilege transferring method for safely transferring access privileges between clients and between clients and servers, over an object space in which at least one server for providing objects and at least one client requiring the objects are connected to one another by a network and access to each of the objects complying with privilege information held by each of the clients is allowed, comprising:

holding user information and secret information by each of a plurality of clients (Figure 1 [blocks 104, 114], 2 [step 204], 6 [step 244], 11 [blocks 1104], column 3, line 62 to column 4, line 3, column 4, lines 29-51, column 5, lines 18-40);

holding in a server, the user information and the secret information of at least a first of the plurality of clients (Figure 1 [block 124], 3 [step 218], 7 [step 262], 11 [blocks 1122, 1123], column 3, line 62 to column 4, line 3, column 4, line 51 to column 5, line 18, column 5, lines 28-51);

generating privilege information by the at least the first of the plurality of clients (Figure 2 [step 208], 3 [steps 214, 216], 6 [steps 246, 248], 7 [steps 258, 260], column 4, lines 42-63, column 5, lines 18-40);

applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating first protected privilege information by the at least the first of the plurality of clients (Figure 2 [step 208], 3 [steps 214, 216], 6 [steps 246, 248], 7 [steps 258, 260], column 4, lines 42-63, column 5, lines 18-40);

transmitting the user information, the privilege information and the first protected privilege information from the at least the first of the plurality of clients to at least a second of the plurality of clients (Figure 9 [block 286], column 5, line 62 to column 6, line 12);

applying the predetermined calculating operation to information comprising at least the challenge character string and the first protected privilege information, thereby generating second protected privilege information by the at least the second of the plurality clients ();

transmitting the user information, the privilege information and the second protected privilege information from the at least the second of the plurality clients to the server, thereby making a request to access and object (Figure 9 [block 288], column 5, line 62 to column 6, line 12);

checking, by the server, whether the privilege information received by the server is valid (column 6, lines 29-47);

comparing the received second protected privilege information with the generated second protected privilege information (Figure 9 [steps 290, 292], column 5, line 62 to column 6, line 12); and

allowing access to the object in response to the coincidence of the received second protected privilege information and the generated second protected privilege information based on the results of the comparison (Figure 9 [step 296], column 6, lines 9-28, column 14, lines 3-51, i.e. accessing objects via the object request broker).

22. Madoukh does not disclose applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege by the server; receiving, by the at least the second of the plurality clients, a challenge character string from the server; applying the predetermined calculating operation to information comprising at least the challenge character string and the generated first protected privilege information thereby generating second protected privilege information.

23. Krahn teaches hashing a password and comparing it against stored hashed passwords (column 1, line 53 to column 2, line 13).

24. It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply a predetermined calculation to the information (i.e. one-way hash) and comparing the protected information with the generated protected information, since Krahn states at column 2, lines 9-12 that the server does not store plain-text passwords, thereby preventing unauthorized access from obtaining every user's password.

25. Perlman discloses receiving, by the at least the second of the plurality clients, a challenge character string from the server (Figure 7 [block 700], column 11, lines 7-20);

applying the predetermined calculating operation to information comprising at least the challenge character string and the generated first protected privilege information thereby generating second protected privilege information (Figure 7 [blocks 730, 740], column 11, lines 7-20).

26. It would have been obvious to one of ordinary skill in the art at the time the invention was made to provide a second level of authentication and share the authentication information, since Perlman states at column 2, lines 47-67 that such a modification would allow two computers with a shared secret to establish a stronger shared secret without risking attacks on the shared secrets, shared secret key exchange protocols also strengthen password based systems by avoiding sending the password in the clear.

27. As per claims 8 and 14, Madoukh teaches an access privilege transferring method for safely transferring access privileges between clients and servers to which user information, privilege information and first protected privilege information are transferred, over an object space in which at least one server for providing objects and at least one client f-requiring the objects are connected to one another by a network and access to each of the objects complying with privilege information held by each of the clients is allowed, comprising:

applying a predetermined calculating operation to information comprising at least the challenge character string and first protected privilege information, thereby generating second protected privilege information by the client (Figure 2 [step 208], 3 [steps 214, 216], 6 [steps 246, 248], 7 [steps 258, 260], column 4, lines 42-63, column 5, lines 18-40);

retransmitting by the client, user information, the privilege information and the second protected privilege information to the server, thereby making a request to access an object (Figure 9 [block 288], column 5, line 62 to column 6, line 12);

checking, by the server, whether the privilege information received by the server is valid (column 6, lines 29-47);

comparing, in the server, the second protected privilege information received and checked by the server with the second protected privilege information generated by the server (Figure 9 [steps 290, 292], column 5, line 62 to column 6, line 12);

allowing access to an object by the server in response to the coincidence of the received second protected privilege information and the generated second protected privilege information based on the results of the comparison (Figure 9 [step 296], column 6, lines 9-28, column 14, lines 3-51, i.e. accessing objects via the object request broker).

28. Madoukh does not disclose applying a predetermined calculating operation to information comprising at least the privilege information and the secret information, thereby generating protected privilege by the server; transmitting a challenge character string from the server to a client that makes a request to access an object; applying the predetermined calculating operation to information comprising at least the challenge character string and the first protected privilege information generated by the server, thereby generating second protected privilege information by the server.

29. Krahn teaches hashing a password and comparing it against stored hashed passwords (column 1, line 53 to column 2, line 13).

30. It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply a predetermined calculation to the information (i.e. one-way hash) and comparing the protected information with the generated protected information, since Krahn states at column 2, lines 9-12 that the server does not store plain-text passwords, thereby preventing unauthorized access from obtaining every user's password.

31. Perlman discloses transmitting a challenge character string from the server to a client that makes a request to access an object (Figure 7 [block 700], column 11, lines 7-20);

applying the predetermined calculating operation to information comprising at least the challenge character string and the generated first protected privilege information thereby generating second protected privilege information (Figure 7 [blocks 730, 740], column 11, lines 7-20).

32. It would have been obvious to one of ordinary skill in the art at the time the invention was made to provide a second level of authentication and share the authentication information,

since Perlman states at column 2, lines 47-67 that such a modification would allow two computers with a shared secret to establish a stronger shared secret without risking attacks on the shared secrets, shared secret key exchange protocols also strengthen password based systems by avoiding sending the password in the clear.

Conclusion

33. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

34. The following patents are cited to further show the state of the art with respect to transferring privilege information, such as:

United States Patent No. 5,790,667 to Omori et al., which is cited to show sending authentication information to a client and forwarding it to a server.

United States Patent No. 6,799,270 to Bull et al., which is cited to show distributing session keys over a network to each node in a chain of computer nodes.

United States Patent No. 6,269,445 to Nishioka et al., which is cited to show sending authentication information to a client and forwarding it to a server.

United States Patent No. 6,064,736 to Davis et al., which is cited to show two-party key authentication provide additional security against intruders that might gain access to the password database.

United States Patent No. 6,519,647 to Howard et al., which is cited to show synchronizing access control in a web server.

United States Patent No. 5,774,552 to Grimmer, which is cited to show retrieving, verifying, and using information accessible by a directory service agent to authenticate electronic messages.

35. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

36. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

37. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

38. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

39. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131
Clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100